MICRO FOCUS

NetIQ® Identity Manager

SCIM Driver Deployment Guide for Keeper Password Manager & Digital Vault

August 2020

Legal Notice

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About This Guide

This guide explains how to install and configure the SCIM driver to establish connectivity between Identity Manager and Keeper Password Manager & Digital Vault (also referred as Keeper Application or Keeper in this guide). The guide includes the following information:

- Chapter 1, “Deploying SCIM Driver For Keeper Password Manager & Digital Vault,” on page 9

Audience

This guide is intended for administrators implementing Identity Manager, application server developers, Web services administrators, and consultants. You should also have an understanding of DSML/SPML, SCIM, JSON, and HTML.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For more information about the library for Identity Manager, see the following resources:

- Identity Manager documentation website (https://www.netiq.com/documentation/identity-manager-48/)
- Identity Manager drivers documentation website (https://www.netiq.com/documentation/identity-manager-48-drivers/)

1 Deploying SCIM Driver For Keeper Password Manager & Digital Vault

You can configure a SCIM driver in Identity Manager to connect to external applications complying to SCIM. The following section explains how to setup and configure the SCIM Driver for Keeper Password Manager and Digital Vault (also referred as Keeper Application or Keeper in the following sections).

Installing the SCIM Driver Files and Packages

To start with installing the driver, you must first download and install the driver files and packages to set up the SCIM driver. This section explains procedures to install the driver files and the required driver packages.

Installing the Driver Files

You can install the SCIM driver files as a root user or as a non root user in your system. The procedure to install the driver files is similar for any connected application.

You must ensure that you have the required SCIM drivers files such as,**`.zip`**,**`.rpm`**, **`and`**.**`jar`** etc,. handy to install the SCIM driver in your system.

For example:

- `.zip` file: `NIdm_Driver_SCIM.zip`
- `.rpm` file: `<netiq-DXMLscim.rpm>`
- `.jar` file: `<SCIMUtils.jar>`

This section explains the procedure to install the driver files.

1. Download and unzip the contents of the **NIdM_Driver_SCIM.zip** file to a temporary location on your computer.
2. To install the driver files as a root user, for IDM 4.7.4 and above:
   - **2a** On the server where you want apply the driver jar file, log in as root.
   - **2b** Navigate to the extracted **NIdM_Driver_SCIM.zip** directory and perform one of the following actions for your platform:
     - **Linux**: Install the new **netiq-DXMLscim.rpm** in your driver installation directory by running one of the following command in a terminal window:
       - If you are installing the binary, run the command: **rpm -Ivh (binaries-path)/netiq-DXMLscim.rpm**
     - **Windows**: Copy the **SCIMShim.jar** file to the driver's installation folder. For example, **\NetIQ\IdentityManager\NDS** (local installation) or **\Novell\RemoteLoader\64bit** (remote installation).
3. (Conditional) To update the driver files as a non-root user:
   - **3a** Verify that the **/rpm** directory exists and contains the **_db.000** file.

     The **_db.000** file is created during a non-root installation of the Identity Manager engine. The absence of this file indicates that the Identity Manager is not installed properly. In such a case, reinstall the Identity Manager to correctly place the file in the mentioned directory.
   - **3b** To set the root directory to the location of non-root Identity Vault, enter the following command in the command prompt:

     ROOTDIR=<non-root eDirectory location>

     This command sets the environmental variables to the directory to the location where the Identity Vault is installed as a non-root user.
   - **3c** To install the driver files, enter the following command:

     For example, to install the SCIM driver rpm, use this command:

     ```
     rpm --dbpath $ROOTDIR/rpm -Ivh --relocate=/usr=$ROOTDIR/opt/novell/
     eDirectory --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/
     eDirectory=$ROOTDIR/opt/novell/eDirectory --relocate=/opt/novell/
     dirxml=$ROOTDIR/opt/novell/dirxml --relocate=/var=$ROOTDIR/var --
     badreloc --nodeps --replacefiles /home/user/netiq-DXMLscim.rpm
     ```

     NOTE: In the above command **/opt/novell/eDirectory** is the location where non-root Identity Vault is installed, and **/home/user/** is the home directory of the non-root user.
4. (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.
5. (Conditional) If the driver is running with a Remote Loader instance, start the Remote Loader instance and the driver instance.

Extending eDirectory (Identity Vault) Schema

You can upload new attributes through the Identity Vault to extend the SCIM schema.

1. Copy the following schema file to the system where Identity Manager is installed.

For example, **`/root/schema/scim-schema.sch`**

2 Run the following **`ndssch`** command.

`ndssch [-h hostname[:port]] [-t tree_name] [-d] admin_FDN schemafile [schema_description]`

For example, **`ndssch -h 10.71.131.123:524 -t SLES12SP3_Quality_131123_TREE -d admin.sa.system /root/schema/scim-schema.sch scim-Group`**

3 The log file is created in the default location, i.e **`/root/schema.log`** for troubleshooting.

NOTE: You must restart the Identity Vault to see the schema changes.

Installing the Driver Packages in Designer

You must install the SCIM Base and SCIM Default and the configuration packages of the Keeper application mandatorily. The required packages and the versions to be installed are as follows:

- **SCIM Base Package**:
  - **Package Name**: NETQSCIMBASE
  - **Version**: 1.0.0
  - **Build Date**: 20200812
  - **Build Number**: 172426
- **SCIM Default Package**:
  - **Package Name**: NETQSCIMDCFG
  - **Version**: 1.0.0
  - **Build Date**: 20200806
  - **Build Number**: 185236
- **SCIM JSON Package** (Optional):
  - **Package Name**: NETQSCIMJSON
  - **Version**: 1.0.0
  - **Build Date**: 20200721
  - **Build Number**: 184051
- **SCIM KeeperSecurity Configuration Package** (Mandatory):
  - **Package Name**: NETQSCIMKSCG
  - **Version**: 1.0.0
  - **Build Date**: 20200806
  - **Build Number**: 185253

For more information to install the SCIM driver packages in the Designer, see SCIM Driver Packages in "*NetIQ SCIM Driver Implementation Guide*".

Creating SCIM Driver Object for Connecting to Keeper Password Manager and Digital Vault in Designer

To begin with the configuration, you need to set up the SCIM driver object in the designer, and configure the SCIM driver with the specific parameters to connect to Keeper application.

The procedure to set up the SCIM driver in designer is similar for any connected application. The generic steps to set up a driver object in designer is shown from step 1 to step 20, and the configuration parameters specific to Keeper application is mentioned in step 22. If you are familiar with the generic driver object set up, you can choose to skip to Step 22 on page 13 to see the configuration parameters specific to Keeper application.

1. Open Designer.
2. In the toolbar, click **Help** > **Check for Package Updates**.
3. Select the required package to download and click **OK**. The designer is updated with the selected packages. For the packages that need to be selected for Keeper, see "Installing the Driver Packages in Designer" on page 11.
4. In the Outline view, right-click the **Package Catalog**.
5. Click **Import Package** and install the **SCIM KeeperSecurity Configuration Package**.
6. By default, only the base packages are displayed. Deselect **Show Base Packages Only** to display all packages.
7. Scroll to find the required package and select it.
8. Click **OK** to import the selected packages, then click **OK** in the successfully imported packages message.
9. In **Designer > Outline** view, open your project.
10. Right click project > **New** > **Identity Vault**, or drag and drop Identity Vault from the Palette to Modeler window.
11. In the **Add Server Association** screen, select the following field values and click **OK**.
    - Server DN
    - Identity Manager Version
    - Identity Manager Edition

    The Identity Vault Credentials window appears.
12. In Identity Vault Credentials window, enter:

Field	Description
Host	The identity vault hosting machine's IP address
Username	The name of the user, for example, Admin, if the user is an administrator.
Password	The password of the user to login to the identity vault

13. Select **Save Password**, if you want to save your password for easy logins in the future.
14. Click **OK**.

    The Identity Vault with the Driver Set appears in the **Modeler** window.

15 In the right pane, drag and drop the **SCIM** driver icon from **Palette > Tool** tab to the **Modeler** window.

16 In the **Driver Configuration Wizard**, select **SCIM Base** (Contains the base functionality for a driver. You must install a driver base configuration package first).

NOTE: You can only select one base package.

---

17 Click **Next**.

18 In the **Select Mandatory Features** page, select the **SCIM Default Package**, and click **Next**.

19 In the **Select Optional Features** page, select the **SCIM KeeperSecurity Configuration Package**, and if required select **SCIM JSON Package**, and click **Next**.

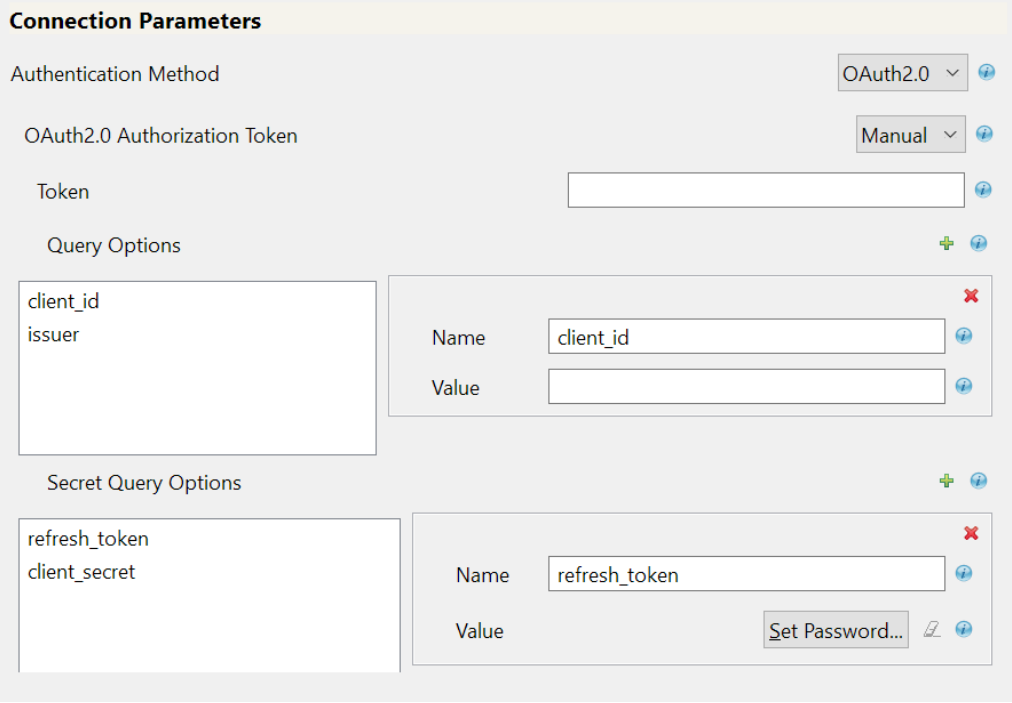
IMPORTANT: Though the **SCIM KeeperSecurity Configuration Package** appears in the **Select Optional Features** page, to configure the SCIM driver for Keeper you must select this package mandatorily.

---

20 Verify if the required **Important Note** items are met, and click **Next**.

21 On the **Driver Information** page, specify a name for the driver, then click **Next**. The **Connection Parameters** page appears.

22 Select **OAuth 2.0** in the **Authentication Method** field, it is recommended to use OAuth2.0 since it is the most secure authentication method.



23 In the **OAuth2.0 Token Management field,** select **Manual**, as the other options JWT and Bearer, are not supported by Keeper application.

The following fields appear:

Field	Field Value
Token: Specify the token generated from the Keeper application. The procedure to generate a token is shown below: 1. Login to Keeper application and navigate to the **Root** node. 2. Select the **User Defined** node. 3. Click **Provisioning** tab. 4. Click **Add Method** and from the options that appear select **SCIM**. 5. Click **Next**, the URL appears. 6. Click **Create Provisioning Token**, the token is generated.	*<9xdQQZzVwvmfe+gIGab0z8VnqlejRDgPgxYtR3bPW7o=>*
Query Options: You can add your query options as per requirement to suit your environment.	Not Applicable for Keeper application. **NOTE:** It is applicable only if new bearer token needs to be generated, and generating a new bearer token is not supported by Keeper application.
Secret Query Options: You can add your query options as per requirement to suit your environment. The values specified in these options are hidden for security purposes.	Not Applicable for Keeper application. **NOTE:** It is applicable only if new bearer token needs to be generated, and generating a new bearer token is not supported by Keeper application.
Application Truststore File: The path and the name of the keystore file, that contains the trusted certificates for the application server or connected system to achieve SSL handshake.	*</root/scim_configuration/trustKeeperSec/KeeperSec>* For more information on how to create the truststore file, see Configuring the Subscriber Channel in "*NetIQ Identity Manager Driver Administration Guide*".
Mutual Authentication	Mutual Authentication is not supported by Keeper application.
Proxy Authentication: Defaults to **Hide**. Select **Show** if you want to set proxy authentication parameters. Specify the host address and the host post when a proxy host and port are used.	◆ **Proxy host name and port**: *<192.168.0.0:port>*. Choose an unused port number on the proxy server. ◆ **Username**: *<user name for proxy authentication>* ◆ **Enter Password**: *<password for proxy authentication>* ◆ **Re-enter Password**: *<password for proxy authentication>*
HTTPS Connection Timeout: Specify the HTTP connection time out value.	The timeout value must be greater than 0. **NOTE:** The driver waits for the time specified (in minutes) and terminates the HTTPS connection displaying the error codes that are configured in the **Subscriber Options > HTTPS error codes for retry** field.

Field	Field Value
SCIM 2.0 URL: Enter the URL for the SCIM Application. SCIM Resources like User, Group etc. will be appended to this URL.	*<https://keepersecurity.com/api/rest/scim/v2/345074852429829/>*

24 In the **Install SCIM Base** page, specify the **Subscriber Options** and **Publisher Options**, and click **Next**.

Field	Description and Sample Values
Subscriber Options	**HTTPS error codes for retry**: Specify the HTTPS errors that must return a retry status. Error codes must be a list of integers separated by spaces. For example: *<307 408 503 504>* **NOTE:** The operation will be retried if these errors are encountered.

Field	Description and Sample Values
Publisher Options	◆ **Enable Publisher Channel**: Select **Yes** to enable the Publisher channel. ◆ **Polling interval in minutes**: Specify the polling interval in minutes For example: *<10>* ◆ **Heartbeat interval in minutes**: This option is used to configure the driver shim to send a periodic status message on the Publisher channel. By default, this is set to 10 minutes. **IMPORTANT: Polling Resource Options**: This field does not appear when you are setting up the driver for the first time. These options are to be specified once the driver is configured. Once the driver is configured, double click the connector line in the modeler window and navigate to **Driver Configuration > Publisher Options** tab. ◆ Select the **Configured Resources** option to poll on all resources that are configured as part of the schema settings. ◆ Select the **Custom Resources** option and click  to configure customized polling **Resource ID** and **Resource URL**. ◆ For User: ◆ **Resource ID**: Example, `urn:ietf:params:scim:schemas:core:2.0:User` ◆ **Resource URL**: Example, `https://keepersecurity.com/api/rest/scim/v2/345074852429829/Users?startIndex=1&count=100` **NOTE:** In the above URL's The `startIndex` refers to the resource from where the poll must start and `count` refers to the number of resources from the `startIndex` for polling. ◆ For Group: ◆ **Resource ID**: Example, `urn:ietf:params:scim:schemas:core:2.0:Group` ◆ **Resource URL**: Example, `https://keepersecurity.com/api/rest/scim/v2/345074852429829/Groups?startIndex=1&count=100`

25 In the **Schema Settings** page, enter the values as shown in the following table:

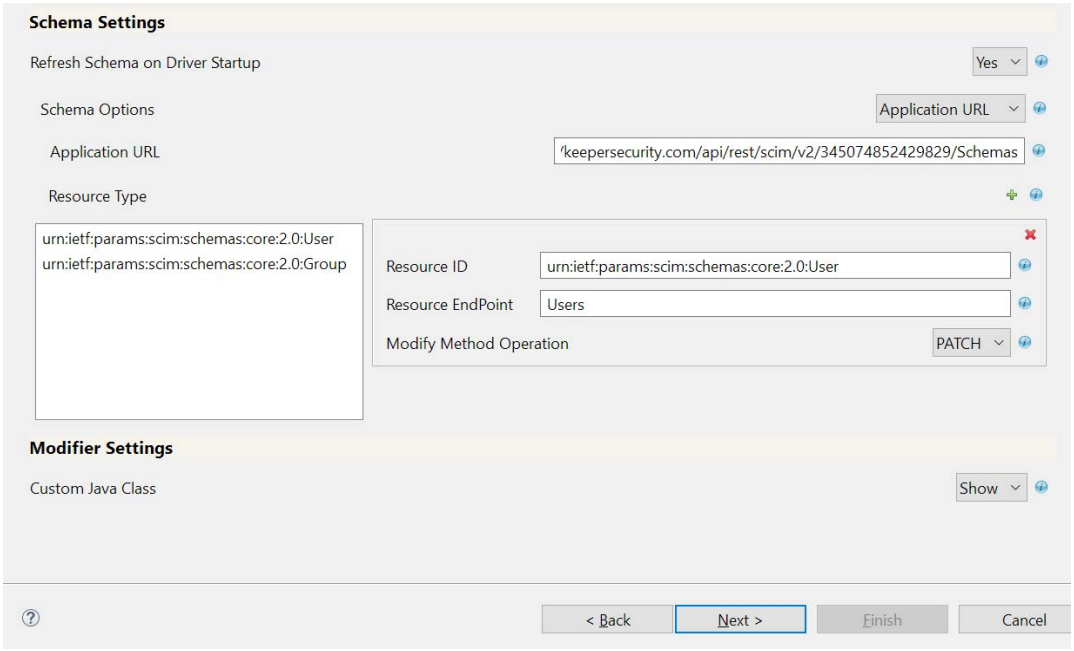


Table 1-1 *Schema Settings*

Field	Description with Sample Values
Refresh Schema on Driver Startup	Specify **Yes**, to refresh the schema. **IMPORTANT:** You must select **Yes** only for the first time to load the application schema or if the application schema has changed. It is recommended to change it to **No** after you load the application schema and if the schema mapping's are completed. For more information see, Refreshing the Fetched Connected Application's Schema in "*NetIQ SCIM Driver Implementation Guide*".
Schema Options	The available options are: ◆ **SCIM 2.0**: SCIM 2.0 Schema for User and Group, as defined in RFC7643. ◆ **Application URL**: Application SCIM Endpoint providing SCIM JSON Schema for Resources like User, Groups, Roles etc. For example, `https://keepersecurity.com/api/rest/scim/v2/345074852429829/Schemas`. ◆ **Import JSON File**: Import the User Defined Schema JSON file from the local file system. This file must comply to SCIM JSON format as per RFC7643. Example, `NIdM_Driver_SCIM\schema\scim_default_schemas`

Field	Description with Sample Values
Resource Type	Specify the Resource ID and Resource EndPoint's for resources like Users, Groups, Roles, Entitlements etc. in Uniform Resource Name (URN) Format. ◆ Resource ID: Resource ID in URN Format. For example, `urn:ietf:params:scim:schemas:core:2.0:Users` ◆ Resource Endpoint: The resource endpoint for the Resource ID. For example, `Users`. ◆ Modify Method Operation: Select PATCH, this option is used to make partial updates of the resource at Keeper. Similarly for Groups: ◆ Resource ID: For example, `urn:ietf:params:scim:schemas:core:2.0:Group` ◆ Resource Endpoint: `Groups` ◆ Modify Method Operation: Select PATCH.

Table 1-2 *Modifier Settings*

Field	Description with Sample Values
Custom Java Class	The custom Java class which is used to extend the driver's functionality. Defaults to Hide, select Show to configure Modifiers.
Document Handling: Defaults to No, select Yes. The **Class** and **Init Parameter** fields appear.	◆ Class: Specify the class using a full package identifier, as shown below, `com.novell.docmodifier.KeeperSecurityDocumentModifiers`. **NOTE:** Ensure the `KSDocMod.jar` file is available in `/opt/novell/eDirectory/lib/dirxml/classes` in Identity Manager. ◆ Init Parameter: Specify the parameters that you want to pass to the init() method of your class, in string format. The init method of your class is responsible for parsing the information contained in this string. Leave this field blank if your class does not require a configuration string to be passed to init method.

26 Review the summary of tasks that will be completed to create the driver, then click Finish. The configured driver appears in the designer screen.

Global Configuration Values

After configuring the SCIM driver, you can set the Global Configuration Values (GCVs) as required. The SCIM driver for Keeper application includes the predefined GCV as shown below:

- **Validate Resource with Required Attributes**: Select as true, to validate resources and the required attributes that are available in the schema.

For more information on GCVs, see When and How to Use Global Configuration Values in "*NetIQ Identity Manager Driver Administration Guide*".

Supported SCIM Driver Use Cases for Keeper Password Manager and Digital Vault

The following operations can be performed on the subscriber channel:

- **Operations performed on a user**
  - **Adding a user**: A user is added in Identity Manager and synced to Keeper through the SCIM driver. The details of the user such as, user's first name, last name, contact details, email ID, location, department, user name, initial login password are added and synchronized to the Keeper application.

    The SCIM end point for Keeper to add a user: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Users`

    Method: POST

    IMPORTANT: Ensure to replace the variable values in the SCIM end point URL as per Keeper specifications. The sample values are shown as follows, and applicable for the SCIM end point examples mentioned in other sections.

    - *<current version>* with *v2,* etc.
    - *<node id>* with *<345074852429829>*
    - *<association>* with *keepersecurity-userid,* or *keepersecurity-groupid,* etc., as applicable.

  - **Modifying a user**: If there are any changes made to the user details such as, user's first name, last name, contact details, email ID etc, they will be synchronized with Keeper application.

    The SCIM end point for Keeper to modify a user: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Users/<keepersecurity-userid>`

    Method: PUT

    NOTE: The user can be disabled in case of separation or termination of their services.

- **Migrate a user**: You can migrate an individual or multiple users from Identity Manager to Keeper application and vice-versa.
- **Polling a user**: You can poll a user from Keeper application to Identity Manager.

  The SCIM end point for Keeper to poll users: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Users`

  Method: GET
- **Query a User**: You can query the synced attributes of resource such as user from Keeper through iManager. Also, we can query through `dxcmd` utility to fetch required resources or attributes using specific conditions.

  The SCIM end point for Keeper to query users: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Users/<keepersecurity-userid>`

Method: GET

NOTE: Complex JSON attributes cannot be queried from SCIM compliant applications through `dxcmd` utility.

- **Operations performed on public groups**
  - **Adding a group**: A group is added in Identity Manager to manage multiple users with same set of access permissions, rather than managing users individually.

    The SCIM end point for Keeper to add a group: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Groups`

    Method: POST
  - **Modifying a group**
    - **Adding member to a group**: A member is added to a group based on the user's role, department and access permissions that the user qualifies for, so that the access permissions for that designated user role are provisioned accordingly.

      The SCIM end point for Keeper to add a member to a group: `https://keepersecurity.com/api/rest/scim/<current version>/<node id>/Groups/<keepersecurity-groupid>`

      Method: POST
    - **Removing member from a group**: A user can be removed from a group if the user's role or designation, or access permissions provided do not qualify a user to belong to that group. This happens in case of a role or designation change of the user, or separation or termination of the user.

      The SCIM end point for Keeper to remove a member from a group: `https://<tenantname>.keepersecurity.com/services/scim/<current version>/<node id>/Groups/<keepersecurity-groupid>`

      Method: POST
  - **Deleting a group**: Duplicate groups, redundant groups, empty groups or groups that are not required can be deleted, and the group members will be moved to another group as required.

    The SCIM end point for Keeper to delete a group: `https://<tenantname>.keepersecurity.com/services/scim/<current version>/<node id>/Groups/<keepersecurity-groupid>`

    Method: DELETE
  - **Migrate a Group**: You can migrate an individual or multiple groups from Identity Manager to the Keeper application and vice-versa.
  - **Polling a Group**: You can poll all created groups from Keeper application to Identity Manager.

    Method: GET

    The SCIM end point for Keeper to poll groups: `<tenantname>.keepersecurity.com/services/scim/<current version>/<node id>/Groups`
  - **Query a Group**: You can query the synced attributes of resource such as group from Keeper through iManager. Also, we can query through `dxcmd` utility to fetch required resources or attributes using specific conditions.

The SCIM end point for Keeper to query groups:
`<tenantname>.keepersecurity.com/services/scim/<current version>/<node id>/Groups`

Method: GET

NOTE: Complex JSON attributes cannot be queried from SCIM compliant applications through `dxcmd` utility.

Known Observations from Keeper Password Manager and Digital Vault

The following are a few observations when some specific operations are performed in Keeper Application.

- For an inactive user, if you modify the username (email id), the display name is updated in the Keeper application.
- If a group is created in Identity Manager and synchronized to Keeper, the display name is blank in the driver log and does not appear in the application.

Mapping Attributes for Keeper Password Manager and Digital Vault

The attributes of Identity Manager and Keeper must be mapped as per the schema mapping. After the schema is fetched from the Keeper application, the attributes of Identity Manager and Keeper are mapped in the backend by default. You can modify the attributes if any changes are required.

For the procedure to modify or change any attribute mapping, see Refreshing the Fetched Connected Application's Schema in "*NetIQ SCIM Driver Implementation Guide*".

You can refer to Mapping Attributes for Identity Manager and Connected Application in "*NetIQ SCIM Driver Implementation Guide*" for the list of attributes that are available for mapping.